

REMARKS/ARGUMENTS

This Amendment is in response to the Final Office Action dated May 25, 2004. Claims 1-42 are pending. Claim 40 has been amended to correct a typographical error that does not change the scope thereof.

Applicant acknowledges the Examiner's indication that Claims 4, 5, 18, 19, 23, 27, and 28 are objected to as being dependent upon a rejected claim, but would be allowable if rewritten in independent form, including all the limitations of the base claim.

The Examiner rejected claims 1-3, 6-17, 20-22, 24-26, and 29-39 under 35 USC §102(b) as being anticipated by Takenaka et al. (US Pat. No. 5,917,908). Applicant respectfully disagrees.

The claims of the present invention recite that a dynamic key used is used to derive an encryption key within a security device. The dynamic key is assigned to software to be protected and does not change between copies of the software. This dynamic key is stored on the security device of the present invention as one of many. Once the protected (encrypted) software is loaded on a computer system and the security device is attached to the computer system and information identifying the software is sent to the security device. The security device uses this information to determine whether the matching dynamic key is present in the security device. Only if the corresponding dynamic key is present does the security device generate the encryption key and send the encryption key to the computer system to unlock the software.

In contrast, Takenaka provides:

A file protection system for protecting a file which is stored in a storage unit includes a storage position deciding unit for deciding a positional-information corresponding to an area in which information of the file is stored in the storage unit and an encryption unit for encrypting the information of the file in accordance with a predetermined algorithm using at least a part of the positional-information decided by the storage position deciding unit. Information obtained by the encryption unit is stored in the area identified by the positional-information in the

storage unit. A file protection system is operable when information of a file which was encrypted as described above is read out from a storage unit. The file protection system includes a decryption unit for decrypting the encrypted information of the file which is read out from an area in the storage unit using information corresponding the area, an extracting unit for extracting the positional-information from information obtained by the decryption unit, and a determination unit for determining whether or not the positional-information extracted by the extracting unit is equal to corresponding positional-information which is at least a part of the information corresponding to the area from which the encrypted information of the file is read out. When the determination unit determines that two pieces of positional-information are not equal to each other, it is determined that the information obtained by the decryption unit does not include correct information of the file. (Abstract)

Takenaka fails to teach or suggest each and every element of the independent claims as there are several differences between the claimed invention and Takenaka's keys and the method Takenaka uses to authenticate the software. First and foremost, Takenaka fails to disclose the use of "an external security device" that is "coupled to the computer system," as recited in claim 1. Takenaka discloses an "input unit," however, this input unit is presumed to be a keyboard because Takenaka states that the user uses the input unit 30 to input the license key (Col. 6, line 36-37). Takenaka also states that the key (license) is "supplied from an external system" (Col. 3, lines 38-39). However, this external system is a center that sells licenses, rather than an external device, and the user manually inputs to they key to the computer through the input unit 30 (Col. 6, lines 21-39).

Second, the dynamic key of the present invention is assigned to a particular *software product* and used to generate an encryption key to keep the encryption key secret. In the rejection, the Examiner merely cited the abstract of Takenaka and failed to state what keys in Takenaka correspond to the dynamic key and encryption key.

It is respectfully submitted that Takenaka's license key does not teach or suggest the dynamic key. Takenaka provides a protection where files are encrypted based on position in a

storage medium. That means that a file in one position will be encrypted with a different key than a file in another position. The Examiner states that the key does not change between copies of software, but it does, because it is determined based on the file's position in the storage medium. This is unlike the present invention, where the dynamic key is the same in all copies of the software for a particular product.

In addition, Takenaka's "secret" key is simply stored with the encrypted file and not "generated" as the claimed encryption key. Therefore, Takenaka does teach or suggest "generating the encryption key within the security device," as recited in claims 1 and 24. In the present invention, the generation of the encryption key and even the dynamic key itself are kept secret in the security device to prevent hacking.

Not only does Takenaka fail to teach or suggest that the encryption key is generated within the security device, Takenaka also fails to teach or suggest "using information supplied from the software to determine if the dynamic key assigned to the software is present in the security device, and if so, generating the encryption key within the security device using the dynamic key," as recited in claims 1 and 24. Independent claims 16, 22, 24, and 39 have similar recitations.

Takenaka does not teach or suggest the sending any information from the computer system to an attached security device. Referring to claim 22 as a further example, the security key (encryption key in claim 1) is generated using an initialization vector and the dynamic key. The initialization vector is provided with the software and the dynamic key is stored on the security device. During authentication, the initialization vector is *sent from the computer system to the security device*, where it is used with the dynamic key assigned to the software to generate the encryption key. In contrast, none of Takenaka's keys are sent to any security device. As a result, there is no way to generate Takenaka's license key, secret key, or otherwise on the security

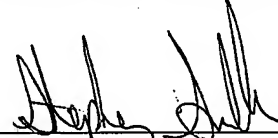
device.

Further, claims 16, 22 and 39, and 40 should be independently allowable as they include additional recitations than claims 1 and 24.

Therefore, for the above identified reasons, the present invention as recited in claims 1-42 is neither taught nor suggested by Takenaka. In view of the foregoing, Applicant submits that claims 1-42 are patentable over the cited reference. Applicant, therefore, respectfully requests reconsideration and allowance of the claims as now presented.

Applicants' attorney believes this application in condition for allowance. Should any unresolved issues remain, Examiner is invited to call Applicants' attorney at the telephone number indicated below.

Respectfully submitted,
SAWYER LAW GROUP LLP



Stephen Sullivan
Sawyer Law Group LLP
Attorney for Applicant(s)
Reg. No. 38,329
(650) 493-4540

July 23, 2004

Date